

Appl. No. 10/798,079
Filed. March 11, 2004
Reply to Office action of September 11, 2006

RECEIVED
CENTRAL FAX CENTER

DEC 08 2006

REMARKS/ARGUMENTS

Claims Remaining

Claims 1-88 remain in the application.

Election of Species Requirement

The examiner has issued an election of species requirement under 35 U.S.C. 121 to one of the inventions claimed in claims 1-88; no claims being deemed generic. The Examiner has required election between thirteen species: (I) claims 1-6, drawn a method for detecting intrusions in a database application, and (II) claims 7-13, drawn to a method for detecting an anomalous command in a database application, and (III) claims 14-21 drawn to a method for detecting attempts to access a database application from invalid sources, and (IV) claims 22-30, drawn to a method for detecting unauthorized activity in a database application, and (V) claims 31-35, drawn to a method for detecting activity designed to breach security of a database application, and (VI) claims 36-39, drawn to a method for detecting suspicious activity in a database application, and (VII) claims 40-41, drawn to a method for detecting use of keywords to suppress auditing of attacks in a database application, and (VIII) claims 42-49, drawn to a method for blocking attacks on database applications, and (IX) claims 50-53, drawn to a method for detecting attempts to inject SQL into a database application, and (X) claims 54-60, drawn to a method for detecting malicious activity in a database application, and (XI) claims 60-63, drawn to a method for detecting activity which may result in cross-site scripting vulnerabilities, and (XII) claims 64-85, drawn to a method for detecting monitoring all activity for security

Appl. No. 10/798,079
Filed. March 11, 2004
Reply to Office action of September 11, 2006

and auditing, and (XIII) claims 86-88, drawn to a method for providing exceptions to security alerts. The Examiner classified each of the thirteen species under class 707, subclass 100. Class 707 refers to "Data Processing: Database And File Management or Data Structures." Subclass 100 refers specifically to "Database Schema or Data Structure."

Applicants provisionally elect to prosecute the species of Group 4, claims 22-30, with traverse.

Groups I, V, VI, VII, IX, XI; claims 1-6, 31-41, 50-52, 60-63, are readable on the provisionally elected claims of Group IV, claims 22-30. They include the basic steps of monitoring SQL statements, actuating database events and analyzing database events.

Groups II, III, VIII, X, XII, XIII; claims 7-21, 42-49, 53-60, 64-88, are not readable on the provisionally claims of Group IV, claims 22-30. They include the additional step of "generating a rule set" or the additional step of "recording" activity in the database.

Listing of Claims Readable Thereon

Applicant lists claims 1-6, 31-41, 50-52, and 60-63. The listing of claims readable thereon are as follows:

Claim 1 (previously presented): A method for detecting attempted intrusions in a database application, the method comprising:

monitoring for an SQL statement, said SQL statement executable in said database application and intended to exploit a vulnerability;
actuating said SQL statement to discover an atomic SQL command;

Appl. No. 10/798,079
Filed. March 11, 2004
Reply to Office action of September 11, 2006

analyzing said atomic SQL command against a pre-defined set of detection rules.

Claim 2 (previously presented): The method according to claim 1, wherein said vulnerability is a buffer overflow in a SQL procedure.

Claim 3 (previously presented): The method according to claim 1, wherein said vulnerability is a buffer overflow in a call from SQL to an operating system function.

Claim 4 (previously presented): The method according to claim 1, wherein said vulnerability is an attempt to escalate privileges of a user in said database application.

Claim 5 (previously presented): The method according to claim 1, wherein said vulnerability is an attempt to escalate privileges within an operating system.

Claim 6 (previously presented): The method according to claim 1, wherein said vulnerability is an attempt to insert an invasive SQL statement into a parameter of stored procedures.

Claim 31 (previously presented): A method for detecting activity designed to breach security of a database application, the method comprising:

monitoring for discrete events executable in said database application and intended to breach a security mechanism associated with said database application;
actuating each discrete database event;

Appl. No. 10/798,079
Filed. March 11, 2004
Reply to Office action of September 11, 2006

analyzing said database events against a pre-defined set of detection rules.

Claim 32 (previously presented): The method according to claim 31, wherein said activity is a brute-force guessing of usernames in said database application.

Claim 33 (previously presented): The method according to claim 31, wherein said activity is the brute-force guessing of usernames and passwords for default accounts in said database application.

Claim 34 (previously presented): The method according to claim 31, wherein said activity is the brute-force guessing of usernames and passwords for well-known accounts in said database application.

Claim 35 (previously presented): The method according to claim 31, wherein said activity is the scripting of password guessing against the database application.

Claim 36 (previously presented): A method for detecting suspicious activity in a database application, the method comprising:

- monitoring for SQL statements executable in said database application which contain characteristics indicative of an attack;

- acruating each batch statement in order to discover atomic SQL commands;

- analyzing said atomic SQL commands against a pre-defined set of rules to identify said suspicious activity.

Appl. No. 10/798,079
Filed. March 11, 2004
Reply to Office action of September 11, 2006

Claim 37 (previously presented): The method according to claim 36, wherein said suspicious activity is a use of comments within an SQL statement.

Claim 38 (previously presented): The method according to claim 36, wherein said suspicious activity is a use of a UNION keyword within an SQL statement.

Claim 39 (previously presented): The method according to claim 36, wherein said suspicious activity is a use of a keyword designed to suppress auditing data.

Claim 40 (previously presented): A method for detecting use of keywords to suppress auditing of attacks in a database application, the method comprising:

- monitoring for SQL statements that contain a keyword, where said keyword results in audit data being suppressed;
- detecting a suppressed SQL statement;
- detecting a conclusion of said suppressed SQL statement;
- determining that no execution of said keyword designed to suppress said SQL statement actually occurred.

Claim 41 (previously presented): The method according to claim 40, further comprising a use of passwords designed to cause an auditing system to suppress text of said SQL statement and masking malicious activity.

Appl. No. 10/798,079

Filed. March 11, 2004

Reply to Office action of September 11, 2006

Claim 50 (previously presented): A method for detecting attempts to inject SQL into a database application, the method comprising:

monitoring for SQL statements executable in said database application and intended to run queries not designed to be run by a middle-tier application;

analyzing said SQL statement's identifying characteristics indicative of SQL injection;

implementing an action upon detection of identifying characteristics indicative of SQL injection.

Claim 51 (previously presented): The method according to claim 50, wherein said action is causing a security alert to be fired.

Claim 52 (previously presented): The method according to claim 50, wherein said action is causing the SQL statement to be blocked.

Claim 60 (previously presented): A method for detecting activity which may result in cross-site scripting vulnerabilities, the method comprising:

monitoring for SQL statements executable in said database application;

actuating each batch statement in order to discover atomic SQL commands;

examining an atomic SQL command for HTML tags.

Claim 61 (previously presented): The method according to claim 60, wherein said atomic SQL command contains an HTML tag.

Appl. No. 10/798,079
Filed. March 11, 2004
Reply to Office action of September 11, 2006

Claim 62 (previously presented): The method according to claim 61, wherein said HTML tag is unencoded.

Claim 63 (previously presented): The method according to claim 61, wherein said HTML tag is hex encoded.

Request for Reconsideration/Traverse

Applicant respectfully suggests that the initial classification of the claimed invention into class 707 subclass 100, respectively "Data Processing: Database and File Management or Data Structures" and "Database Schema or Data Structure", was incorrect. Applicant suggests that the examiner consider class 726 subclass 22, "Information Security" and "Monitoring or Scanning Software or Data Including Attack Prevention" as an appropriate classification. Applicant believes that any burden on the examiner may be removed by reclassifying the invention into the classification suggested above.

CONCLUSION:

Applicants believe that the above is fully responsive to the examiner's concerns, and request withdrawal of the species election requirement.

Appl. No. 10/798,079
Filed. March 11, 2004
Reply to Office action of September 11, 2006

Respectfully submitted,

Law Offices of Peter S. Canelias

December 8, 2006

By: _____



Peter S. Canelias
Reg. No. 40,547
Law Offices of Peter S. Canelias
420 Lexington Avenue-Suite 2148
New York, NY 10170
Tel: (212) 223-9654
Fax: (212) 223-9651